


RESEARCH

Open Access



Secure spatial modulation based on two-dimensional generalized weighted fractional Fourier transform encryption

Yongxin Huang^{1,2}, Xuejun Sha¹, Xiaojie Fang^{1,2*}  and Ge Song¹

*Correspondence:
fangxiaojie@hit.edu.cn

¹ School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China

² Science and Technology on Communication Networks Laboratory, Shijiazhuang 050051, China

Abstract

In this paper, a two-dimensional generalized weighted fractional Fourier transform (2DGWFRFT) and constellation scrambling (CS)-based secure spatial modulation (SM) scheme, called 2DGWFRFT-CS-SM, is proposed to enhance the physical layer security (PLS) of the wireless communication system. The proposed scheme is executed by two steps. In the first step, 2DGWFRFT is implemented as the security kernel for PLS provision. In the second step, the parameters of 2DGWFRFT, regarded as the encryption core, control the antenna number rotation to further enhance the security of the SM modulation symbol. Both the 2DGWFRFT signal generation strategy and the SM system including the transfer process have been elaborated to depict the security mechanism of the proposed scheme. Moreover, we give a key extraction algorithm utilized to generate the parameters, which can help scramble the antenna serial number. From the perspective of signal characteristics, the uniqueness of variation in the constellation has been investigated to outperform other cryptography-based encryption algorithms. Finally, the secrecy rates and the energy efficiency of our proposed scheme are theoretically analyzed and evaluated via Monte Carlo simulations, demonstrating that the proposed scheme can achieve a much higher secrecy capacity than artificial noise schemes without requiring additional jamming power consumption and myriad costs of hardware.

Keywords: Physical layer security, Spatial modulation, Two-dimensional generalized weighted fractional Fourier transform, Secrecy rate, Energy efficiency

1 Introduction

Due to the broadcast nature of the wireless channel, confidential messages can be easily wiretapped by illegitimate receivers, making wireless communications more vulnerable. Traditionally, cryptographic algorithms are the most common way for communication security. However, considering the uniqueness and the inherent security superiority associated with the wireless signal propagation, physical layer security (PLS) is emerging as a promising paradigm to complement the higher layer encryptions for security enhancement [1]. Without relying on upper layers encryption, the inherent randomness of the legitimate link is exploited to prevent eavesdroppers from wiretapping the

confidential information [2]. The current development of wireless physical layer security technology has two main directions: one is to generate, manage and distribute keys based on the physical characteristics of the wireless channel, and the other is based on the secrecy capacity and wiretap channel model proposed by Wyner on the basis of Shannon information theory. Specifically, they can be divided into the following aspects: (a) the corresponding security coding strategy is proposed according to the analysis of various types of wiretap channel models and secrecy capacity performance in different wireless channels based on the information theory [3]; (b) beamforming, artificial noise (AN), and cooperative jamming are used in physical layer security schemes [4]; (c) spatial diversity techniques can improve physical layer security, which takes advantage of multi-antenna diversity, multiuser diversity, and cooperative diversity [5]; and (d) the key generated by the wireless channel characteristics can be exploited to encrypt the message [6].

By taking advantage of signal processing in multiple antenna systems, techniques have been developed to explore the extra degrees of freedom for physical layer security [7]. However, issues such as inter-channel interference, inter-antenna synchronization, and multiple radio frequency (RF) chains make the implementation of these schemes unpractical. Recently, spatial modulation (SM) [8] has drawn gradual attention due to its unique structure and it has been introduced to increase energy efficiency and overcome the issues therein compared with the spatial multiplexing multiple-input multiple-output (MIMO) technique [9]. SM works by mapping a block of information bits into two information-carrying units. The first information-carrying unit is an amplitude/phase modulation (APM) symbol chosen from the signal constellation diagram. The second information-carrying unit is a transmit antenna index chosen, while other transmit antennas are not activated [10].

In the SM PLS literature, precoding techniques are always applied for secure communications. The authors in [11–14] generalized precoding schemes to secure SM with good security performance, which will be described in more detail below. For most conventional precoding-aided SM (PSM) schemes, the antenna indices at the receiver are utilized to carry bits rather than the antenna indices of the transmitter as spatial bits. The optimization of the precoding matrix at the transmitter was to address the issues of preprocessing and detection of PSM signals at the receiver in order to improve bit-error-rate (BER) performance [15]. Additionally, the authors in [11] have proposed a time-varying precoder for the secret PSM, which generated a time-varying interference to the eavesdropper and retained all advantages of PSM at the legal receiver. Then, they also derived the upper bounds for BERs at legal receiver and eavesdropper in the massive MIMO systems in [12] and designed a precoder by jointly minimizing the received power at eavesdropper and maximizing the received power at legal receiver in [13]. The kind of PSM was also extended to secure multiuser MIMO downlink scenario by introducing a scrambling matrix to disturb the eavesdropper [14].

Against this backdrop, conventional PSM schemes' drawbacks are also reflected. On the one hand, many of them merely rely on AN, which may result in low energy efficiency since a fraction of the transmit power has to be allocated to the AN. On the other hand, some assumptions, such as the perfect channel state information at the transmitter or the transmitter's antennas outnumber eavesdroppers' to create a null space for

jamming, that are adopted in the information-theoretic secrecy schemes but are not pragmatic to be implemented. Last but not least, the precoding embedded AN scheme demands that all antennas must be turned on at the same time, which is contrary to the original design intention of only one active transmit antenna for SM at each time instant. Meanwhile, this also makes SM directly no different from traditional MIMO, losing its advantages in energy efficiency and material hardware.

One potential solution to address the preceding issues is weighted fractional Fourier transform (WFRFT). WFRFT, known as a novel time–frequency analyzing tool, has been widely applied to wireless PLS transmissions [16–18]. Instead of dissipating additional transmission power for friendly jamming, by leveraging the features of WFRFT, the information-bearing signal itself can create an identical AN effect at the eavesdropper while causing no performance degradation on the legitimate receiver. The WFRFT-based system was pioneeringly proposed in [19] and then extended into multi-parameter WFRFT in [20]. Despite multiple versions of WFRFT, e.g., multiple parameters WFRFT and general multifractional FRFT, which have been defined to meet different security requirements, the core security mechanism is identically derived from [21]. In particular, the security parameters of existing WFRFT-based PLS schemes are determined by a single parameter α only, which significantly limits the security performance of existing schemes.

A novel two-dimensional generalized weighted fractional Fourier transform (2DGWFRFT) and constellation beguiling-based secure SM scheme is proposed in this paper. In the first stage, compared with the traditional WFRFT, by multiple times transformations with different horizontal and vertical dimensions, 2DGWFRFT can further enhance its anti-scanning ability. Inspired by the generalized weighted fractional Fourier transform (GWFRFT) proposed in [22, 23], we remove all frequency-domain components on the basis of WFRFT to form the 2DGWFRFT that only contains time-domain components and thereby adapts the traditional single-link single-carrier spatial modulation. In the second stage, the parameter of the 2DGWFRFT, as the security crux, is generated by the instantaneous channel state over the legitimate link and then exploited to randomize the antenna serial number. Simulation results show that the 2DGWFRFT has all of the desired advantages of the WFRFT, such as requiring no extra jamming signals and confounding the eavesdropper while imposing no impact on the communication of the partner.

The novelty and contribution of this paper are highlighted as follows:

- We propose a novel 2DGWFRFT scheme for SM with antenna encryption. This scheme uses the antenna index rotation created by 2DGWFRFT parameters to protect the spatial constellation diagram, the invertibility, and uniqueness of which effectively protect the confidential messages from being intercepted by the eavesdroppers while imposing no performance degradation on the legitimate receiver.
- Combining the technique of secret keys extraction based on the wireless channel, in the antenna index rotation stage an algorithm for secret keys generation is proposed.
- We study the constellation rotation law about GWFRFT and give the special constellation of 2DGWFRFT for constellation deception.

- We conduct simulations and give a detailed analysis of security rate and efficiency to illustrate the merits of our scheme.

The rest of this paper is organized as follows. Section 2 presents the definition of WFRFT and the generation method of GWFRFT. In the sequel, Sect. 3 depicts the theoretical model of our proposed system. The secure strategy including 2DGWFRFT and antenna number rotation is described in Sect. 4. We analyze the secrecy mutual information and constellation rotation pattern in Sect. 5. In Sect. 6, the numerical results are shown. Finally, Sect. 7 contains the conclusion.

2 Preliminaries

2.1 Definition of the WFRFT

First of all, we give the definition of one-dimensional 4-WFRFT here. An α order WFRFT of any complex vector \mathbf{b} of length N can be expressed as [19]

$$\mathcal{F}^\alpha[\mathbf{b}] = \mathbf{F}^\alpha \mathbf{b} = (\omega_0^\alpha \mathbf{I}_N + \omega_1^\alpha \mathbf{F} + \omega_2^\alpha \mathbf{T} + \omega_3^\alpha \mathbf{TF})\mathbf{b}, \tag{1}$$

where \mathbf{F}^α is the α order $N \times N$ WFRFT matrix and \mathbf{F} denotes the $N \times N$ unitary Fourier matrix satisfying $[\mathbf{F}]_{k,m} := (1/\sqrt{N})\exp(-2\pi km\sqrt{-1}/N)$. \mathbf{I}_N is the $N \times N$ identity matrix and \mathbf{T} is the shift matrix satisfying $[\mathbf{T}]_{k,m} = \delta(\langle k+m \rangle_N)$, where $\langle \cdot \rangle_N$ denotes modulo- N calculation. The weighting coefficients ω_l^α ($l = 0, 1, 2, 3$) are defined as [19]

$$\omega_l^\alpha = \frac{1}{4} \sum_{m=0}^3 \exp \left[\frac{2\pi(\alpha - l)m\sqrt{-1}}{4} \right] \quad (l = 0, 1, 2, 3). \tag{2}$$

2.2 GWFRFT

GWFRFT is equivalent to a generalization of the classical WFRFT-based hybrid carrier system whose purpose is to achieve equal component power. As (1) shows, the classical WFRFT signal can be expressed as a weighted sum of four state functions. Likewise, GWFRFT can be seen as a relaxed version of WFRFT, which is described in [23] as

$$\mathcal{F}^\pm[\mathbf{b}] = (\omega_0^\pm \mathbf{I}_N + \omega_1^\pm \mathbf{F} + \omega_2^\pm \mathbf{T} + \omega_3^\pm \mathbf{TF})\mathbf{b}, \tag{3}$$

where,

$$\begin{cases} \omega_0^\pm = \frac{1}{4}(e^{\pm\phi_0 i} + e^{\pm\phi_1 i} + e^{\pm\phi_2 i} + e^{\pm\phi_3 i}) \\ \omega_1^\pm = \frac{1}{4}(e^{\pm\phi_0 i} - e^{\pm\phi_1 i} - e^{\pm\phi_2 i} + e^{\pm\phi_3 i}) \\ \omega_2^\pm = \frac{1}{4}(e^{\pm\phi_0 i} - e^{\pm\phi_1 i} + e^{\pm\phi_2 i} - e^{\pm\phi_3 i}) \\ \omega_3^\pm = \frac{1}{4}(e^{\pm\phi_0 i} + e^{\pm\phi_1 i} - e^{\pm\phi_2 i} - e^{\pm\phi_3 i}), \end{cases} \tag{4}$$

\mathbf{I}_N , \mathbf{F} , \mathbf{T} and \mathbf{b} have the same physical meaning as the variables in (1); ϕ_l is an eigenvalue whose value is specified in [22]; and ω_l ($l = 0, 1, 2, 3$) is the weighted coefficient of the basis function. + and - present positive and inverse transformation, respectively. Note that GHC could be reduced to the 4-WFRFT when $\phi_l = \pi l\alpha/2$.

For the frequency selected channels, if the frequency-domain components are suppressed and two time-domain components are retained, the transmitted signal power will be better averaged in the time domain, which is beneficial to suppress selective fading in the frequency domain. In order to achieve the above purpose, GWFRFT is introduced into the diversity method design [22, 23]. For the time dispersion channel, the weighted coefficient of the frequency-domain signal is set to be zero by adjusting ϕ_l , i.e., $\omega_l^\pm = \omega_3^\pm = 0$. In the period $[0, 2\pi)$, the solution is $\phi_0 = \phi_2, \phi_1 = \phi_3$, and the weighting coefficients are expressed as $\omega_0^\pm = (e^{\pm\phi_0 i} + e^{\pm\phi_1 i})/2$ and $\omega_2^\pm = (e^{\pm\phi_0 i} - e^{\pm\phi_1 i})/2$. In this way, the formulas of the generalized hybrid carrier (GHC) system signals containing only time-domain components are obtained. In our case, this method contributes to us stifling frequency-domain components and provides us opportunities to design signals other than AN to better fit SM's single-link structures.

3 2DGWFRFT-CS-SM system

We consider the communication model that a transmitter (Alice) sends information to an intended receiver (Bob) in the presence of a passive eavesdropper (Eve). The numbers of antennas equipped by Alice, Bob, and Eve are N_t, N_r , and N_e , respectively. Alice can use the index of transmit antenna (TA) combination to convey $k_1 = \lfloor \log_2(|\mathcal{C}|) \rfloor$ bits, where the set \mathcal{C} includes all combinations associated with choosing 1 TA from N_t TAs. Furthermore, we use $\mathcal{C}(l)$ to represent the l th combination pattern, $l \leq l \leq L = 2^{k_1}$. In addition, another $k_2 = \log_2 M$ bits are conveyed by M -ary APM symbols $b_m \in \mathfrak{B} = b_1, b_2, \dots, b_M$, where \mathfrak{B} denotes the symbol set and $\mathbb{E}[|b_m|^2] = 1, \forall m \in [1, M]$.

3.1 System model

The original symbol can then be represented by [11]

$$s_m^l = \Omega_l b_m, \tag{5}$$

where $\Omega_l = I[:, \mathcal{C}(l)] \in \mathbb{C}^{N_r \times 1}$ is composed of specific columns contained in $\mathcal{C}(l)$ extracted from the identity matrix \mathbf{I} . Note that the antenna rotation begins after each SM symbol performs 2DGWFRFT, of which a specific security strategy will be described in detail in the next section. Therefore, the transmit block can be

$$\mathbf{X} = [s_{1m}^{l_r}, s_{2m}^{l_r}, \dots, s_{Km}^{l_r}] = \Omega_{l_r} \mathcal{F} 2DGWFRFT(b_m), \tag{6}$$

where K is the number of subcarriers. l represents the original antenna serial number, while l_r represents the antenna serial number after encryption and rotation.

As shown in Fig. 1, the received signals are sent into the symbol detector, where the optimal ML criterion is applied in our analysis. The outputs of the detector are operated by spatial demodulation, and further, the transmitted bit information is recovered. The inverse 2DGWFRFT is run in the ML detector.

For the legitimate receiver Bob and the eavesdropper Eve, the received signals are, respectively, expressed as

$$\mathbf{Y}_b = \mathbf{H}_b \mathbf{X} + \mathbf{W}_b, \tag{7}$$

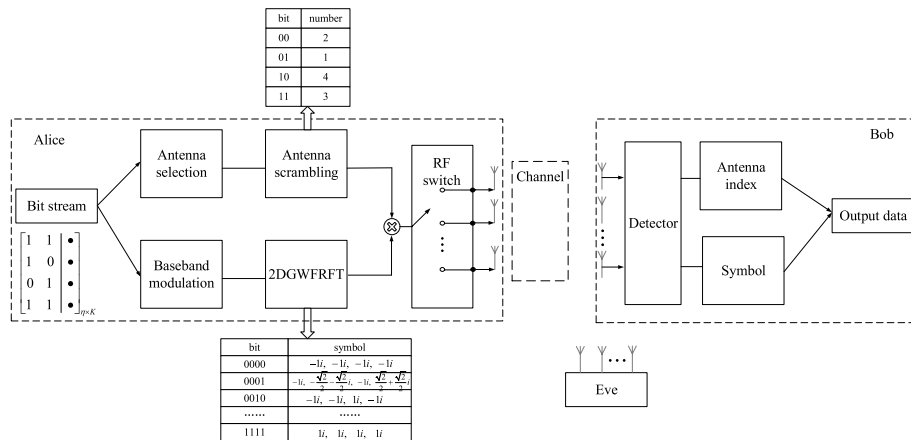


Fig. 1 Basic structure of the proposed system model

$$\mathbf{Y}_e = \mathbf{H}_e \mathbf{X} + \mathbf{W}_e, \tag{8}$$

where $\mathbf{H}_b \in \mathbb{C}^{N_r \times N_t}$ and $\mathbf{H}_e \in \mathbb{C}^{N_e \times N_t}$ represent the Rayleigh flat fading channel matrices from Alice to Bob and Eve, respectively. $\mathbf{W}_b = [\epsilon_{b1}, \epsilon_{b2}, \dots, \epsilon_{bK}]$, $\mathbf{W}_e = [\epsilon_{e1}, \epsilon_{e2}, \dots, \epsilon_{eK}]$, where $\epsilon_{bi} \in \mathbb{C}^{N_b \times 1}$ and $\epsilon_{ei} \in \mathbb{C}^{N_e \times 1}$ are complex Gaussian noise vectors with zero mean and covariance matrix $\sigma_b^2 \mathbf{I}_{N_r}$ and $\sigma_e^2 \mathbf{I}_{N_e}$, respectively. In this case, as Bob shares the parameter information with Alice, Bob can recover the information through the optimal maximum likelihood (ML) algorithm as follows:

$$(\hat{l}, \hat{m}_1, \dots, \hat{m}_K) = \arg \min_{\forall m_i \in [1, M], l \in [1, L]} \left\{ \|\mathbf{Y}_b - \mathbf{H}_b \mathbf{X}\|^2 \right\}. \tag{9}$$

For the eavesdropper, here we assume: (a) Eve has already obtained the channel state information between Alice and Bob whilst Eve can steal the feedback link or Eve is located very close to Bob. (b) Eve is familiar with 2DGWFRFT but not the accurate parameter. Therefore, Eve may employ the ML algorithm:

$$(\hat{l}, \hat{m}_1, \dots, \hat{m}_K) = \arg \min_{\forall m_i \in [1, M], l \in [1, L]} \left\{ \|\mathbf{Y}_e - \mathbf{H}_e \mathbf{X}\|^2 \right\}. \tag{10}$$

4 Secure strategy

4.1 2DGWFRFT

Since the SM system is suitable for the system characteristics of a single carrier and a large bandwidth [24, 25], in the previous section, in order to adapt this characteristic, we eliminated the frequency-domain component in the WFRFT to form the GWFRFT, which is described as:

$$\mathcal{F}_{\text{GWFRFT}}[\mathbf{b}] = \mathbf{G}_{\text{GHC}} \mathbf{b} = (\omega_0^+ \mathbf{I}_N + \omega_2^+ \mathbf{T}) \mathbf{b}, \tag{11}$$

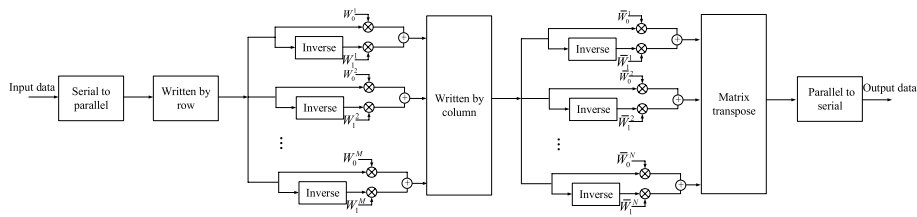


Fig. 2 Schematic of the proposed 2DGWFRFT

Fully utilizing the structural characteristics of GWFRFT time-domain dual signals, AN injection caused by full-antenna transmission can be avoided, thereby improving energy efficiency. At the same time, it also provides the possibility for the extension of parameter degrees for security and confidentiality. This is where we come up with the 2DGWFRFT.

As shown in Fig. 2, 2DGWFRFT can be regarded as a mathematical transformation of GWFRFT for each row and column of the data matrix. It should be noted that it's extremely difficult to get the expression for the 2DGWFRFT with arbitrary vector $W_0, W_2, \bar{W}_0, \bar{W}_2$. However, if the weighted transformation parameters of each row and each column have the same value, i.e.,

$$\begin{cases} W_0^1 = W_0^2 = \dots = W_0^M = \frac{1}{2}(e^{\phi_0 i} + e^{\phi_1 i}) \\ W_2^1 = W_2^2 = \dots = W_2^M = \frac{1}{2}(e^{\phi_0 i} - e^{\phi_1 i}) \\ \bar{W}_0^1 = \bar{W}_0^2 = \dots = \bar{W}_0^N = \frac{1}{2}(e^{\bar{\phi}_0 i} + e^{\bar{\phi}_1 i}) \\ \bar{W}_2^1 = \bar{W}_2^2 = \dots = \bar{W}_2^N = \frac{1}{2}(e^{\bar{\phi}_0 i} - e^{\bar{\phi}_1 i}), \end{cases} \quad (12)$$

the 2DGWFRFT has a simple expression similar to (11). Assume the 2DGWFRFT signal as $\mathbf{k} = [k_0, k_1, \dots, k_{K-1}]^T$. Define the $K \times K$ permutation matrix as

$$\mathbf{P}_{N,M} = \begin{bmatrix} \mathbf{I}_N \otimes i_M^T(0) \\ \mathbf{I}_N \otimes i_M^T(1) \\ \vdots \\ \mathbf{I}_N \otimes i_M^T(M-1) \end{bmatrix},$$

where \mathbf{I}_N denotes the $N \times N$ identity matrix, \otimes denotes the Kronecker product, and $i_M^T(m)$ denotes the m th column vector of \mathbf{I}_M . Then, the transmitted signal \mathbf{k} can be expressed as

$$\begin{aligned} \mathbf{k} &= \mathcal{F}_{2DGWFRFT}(\mathbf{b}) \\ &= \mathbf{P}_{N,M}^H (\mathbf{I}_M \otimes \mathbf{G}_{GHC-N}^{\bar{\phi}_0, \bar{\phi}_1}) \mathbf{P}_{N,M} (\mathbf{I}_N \otimes \mathbf{G}_{GHC-M}^{\phi_0, \phi_1}) \mathbf{b} \\ &= (\mathbf{G}_{GHC-N}^{\bar{\phi}_0, \bar{\phi}_1} \otimes \mathbf{I}_M) (\mathbf{I}_N \otimes \mathbf{G}_{GHC-M}^{\phi_0, \phi_1}) \mathbf{b} \\ &= (\mathbf{G}_{GHC-N}^{\bar{\phi}_0, \bar{\phi}_1} \otimes \mathbf{G}_{GHC-M}^{\phi_0, \phi_1}) \mathbf{b}. \end{aligned} \quad (13)$$

where $(\mathbf{I}_N \otimes \mathbf{G}_{GHC-M}^{\phi_0, \phi_1})$, $\mathbf{P}_{N,M}$, $(\mathbf{I}_M \otimes \mathbf{G}_{GHC-N}^{\bar{\phi}_0, \bar{\phi}_1})$ and $\mathbf{P}_{N,M}^H$ correspond to the row-wise precoding of $\mathbf{G}_{GHC-M}^{\phi_0, \phi_1}$, the row-wise write, the column-wise precoding of $\mathbf{G}_{GHC-N}^{\bar{\phi}_0, \bar{\phi}_1}$ and the row-wise read operations, respectively.

Similarly, the inverse transformation expression is:

$$\begin{aligned}
 \mathbf{b} &= \mathcal{F}_{2\text{DGWFRFT}}(\mathbf{k}) \\
 &= (\mathbf{I}_N \otimes \mathbf{G}_{\text{GHC-M}}^{-(\phi_0, \phi_1)}) \mathbf{P}_{N,M}^H (\mathbf{I}_M \otimes \mathbf{G}_{\text{GHC-N}}^{-(\bar{\phi}_0, \bar{\phi}_1)}) \mathbf{P}_{N,M} \mathbf{k} \\
 &= (\mathbf{I}_N \otimes \mathbf{G}_{\text{GHC-M}}^{-(\phi_0, \phi_1)}) (\mathbf{G}_{\text{GHC-N}}^{-(\bar{\phi}_0, \bar{\phi}_1)} \otimes \mathbf{I}_M) \mathbf{k} \\
 &= (\mathbf{G}_{\text{GHC-N}}^{-(\bar{\phi}_0, \bar{\phi}_1)} \otimes \mathbf{G}_{\text{GHC-M}}^{-(\phi_0, \phi_1)}) \mathbf{b}.
 \end{aligned} \tag{14}$$

4.2 Antenna number rotation

Herein, we elaborate on the antenna scrambling process with reference to Fig. 3. We denote the original antenna index vector without antenna scrambling as Ω_l , which is the l th column of the identity matrix \mathbf{I} , and hence the process of selecting a new antenna index vector is as follows:

- Step 1** First, we can extract the secret key by channel probing [26], measurements quantization [27, 28], information reconciliation [29], and privacy amplification [30]. Bits with common information are subsequently utilized to create parameters that dominate the 2DGWFRFT for secure communication. And the parameters will be updated in real-time as the channel detection changes.
- Step 2** It is necessary to select Nt pairs from the $M + N$ pairs applied to Fig. 2 as the parameter keys, and this set can be expressed as $(\Phi_0^1, \Phi_1^1), \dots, (\Phi_0^l, \Phi_1^l), \dots, (\Phi_0^{Nt}, \Phi_1^{Nt})$.
- Step 3** Calculate their numerical parameters separately and sort them by size, rename them to $|\lambda_1|^2, \dots, |\lambda_l|^2, \dots, |\lambda_{Nt}|^2$, i.e., $|\lambda_1|^2 = \min \left\{ \left| \frac{\Phi_0^1}{\Phi_1^1} \right|^2, \dots, \left| \frac{\Phi_0^l}{\Phi_1^l} \right|^2, \dots, \left| \frac{\Phi_0^{Nt}}{\Phi_1^{Nt}} \right|^2 \right\}$,

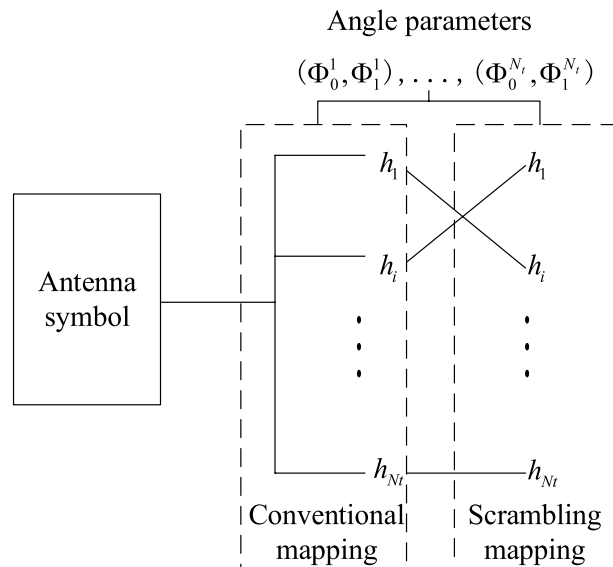


Fig. 3 Scrambling mapping design

$$|\lambda_{Nt}|^2 = \max \left\{ \left| \frac{\Phi_0^1}{\Phi_1^1} \right|^2, \dots, \left| \frac{\Phi_0^l}{\Phi_1^l} \right|^2, \dots, \left| \frac{\Phi_0^{Nt}}{\Phi_1^{Nt}} \right|^2 \right\}. \text{ So that we have } |\lambda_1|^2 \leq \dots \leq |\lambda_l|^2 \leq \dots \leq |\lambda_{Nt}|^2.$$

Step 4 The scrambling mapping is performed in the form of $\Omega_l \rightarrow \left| \frac{\Phi_0^l}{\Phi_1^l} \right|^2 \rightarrow |\lambda_l|^2 \rightarrow \Omega_{lr}$. For example, the original antenna index information bit is 00, the original antenna index activation vector is $\Omega_l = [1, 0, 0, 0]^T$ (that means the first antenna is activated for transmission), and $\left| \frac{\Phi_0^l}{\Phi_1^l} \right|^2$ is ranked second according to the selected key. Hence, the new index vector after scrambling mapping is $\Omega_{lr} = [0, 1, 0, 0]^T$.

Unlike the physical layer security schemes with precoding or artificial noise injection, the proposed mapping-varied spatial modulation does not engage the random channel properties of the legitimate link in the transmitted signal shaping but utilizes the randomness of channel state patterns over the legitimate link to vary the information parameter key at the transmitter. The fundamental advantages behind this scheme are twofold: (1) No artificial noise is injected at the transmitter. As such, the transmit power is fully taken by useful information and high energy efficiency is achieved, which will be formulated in Sect. 5.3. (2) The decoding complexity at the legitimate receiver is the same as that of the classical SM. Therefore, the confidentiality of information transmission can be further improved while the advantages of the existing SM system have been retained without requiring more physical resources or computational complexity.

5 Performance evaluation

5.1 Analysis of secrecy capacity

According to (9), the proposed scheme viewed from Bob represents a special channel, the input symbols \mathbf{X} of which are discrete with finite alphabets, and the output signals \mathbf{Y}_b of which are continuous. Such discrete-input continuous-output memoryless channels, although lacking a closed-form expressions for evaluation of their capacity, can be readily satisfied in a practical communication system [31]. First, the conditional probability distribution function (PDF) of y_b can be expressed as

$$p(y_b | s_{km}^{lr}) = \frac{1}{(\pi \sigma_b^2)^{Nr}} \exp \left(\frac{-\|y_b - s_{km}^{lr}\|^2}{\sigma_b^2} \right). \tag{15}$$

Since lr and km are uniform distributed, the PDF of y_b can be expressed as

$$p(y_b) = \frac{1}{NtM} \sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} \times \left[\frac{1}{(\pi \sigma_b^2)^{Nr}} \exp \left(\frac{-\|y_b - s_{km}^{lr}\|^2}{\sigma_b^2} \right) \right]. \tag{16}$$

Let $s_{m,l}^{n,k} = s_{km}^{lr} - s_{kn}^{kr}$, $n \in [1, M^{Ns}]$, $k \in [1, L]$. Then, we obtain Bob's mutual information as

$$\begin{aligned}
 & I(y_b; s_{km}^l) \\
 &= \int \sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} p(y_b, s_{km}^l) \log_2 \frac{p(y_b, s_{km}^l)}{p(y_b)p(s_{km}^l)} dy_b \\
 &= \frac{1}{MNt} \sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} \int p(y_b | s_{km}^l) \log_2 \frac{p(y_b | s_{km}^l)}{p(y_b)} dy_b \\
 &= \log_2 MNt - \frac{1}{MNt} \sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} \int p(y_b | s_{km}^l) dy_b \\
 &\quad \times \log_2 \left(\frac{\sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} p(y_b | s_{km}^l)}{p(y_b | s_{km}^l)} dy_b \right) \\
 &= \log_2 MNt - \frac{1}{MNt} \sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} \mathbb{E}_{\mathbf{H}_b, \varepsilon_b} \\
 &\quad \times \left[\log_2 \left(\sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} \exp \left(\frac{-\|s_{m,l}^{n,k} + \varepsilon_b\|^2 + \|\varepsilon_b\|^2}{\sigma_b^2} \right) \right) \right].
 \end{aligned} \tag{17}$$

As stated in Sect. 3, since Eve does not know the parameter, she cannot get the correct antenna rotation value and constellation rotation value. Therefore, we have

$$p(h_b = h_e | y_e) = p(l = \hat{l}_e) = p(h_b) = \frac{1}{Nt}, \tag{18}$$

$$p(s_m = s_e | y_e) = p(m = \hat{m}_e) = p(s_m) = \frac{1}{M}, \tag{19}$$

Considering (8) and (10), it is easy to get

$$\begin{aligned}
 p(s_{km}^l | y_e) &= p(l = \hat{l}_e, m = \hat{m}_e | y_e) \\
 &= p(l = \hat{l}_e) p(m = \hat{m}_e) \\
 &= \frac{1}{NtM} = p(s_{km}^l),
 \end{aligned} \tag{20}$$

Multiplying both sides of (20) by $p(y_e)$ yields

$$p(y_e, s_{km}^l) = p(y_e)p(s_{km}^l), \tag{21}$$

Then, we have Eve’s mutual information as

$$\begin{aligned}
 & I(y_e; s_{km}^l) \\
 &= \int \sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} p(y_e, s_{km}^l) \log_2 \frac{p(y_e, s_{km}^l)}{p(y_e)p(s_{km}^l)} dy_e \\
 &= \int \sum_{n=0}^{Nt-1} \sum_{m=0}^{M-1} p(y_e, s_{km}^l) \log_2 \frac{p(y_e)p(s_{km}^l)}{p(y_e)p(s_{km}^l)} dy_e \\
 &= 0.
 \end{aligned} \tag{22}$$

Consequently, the ergodic secrecy rate (SR) can be expressed as [32]

$$\begin{aligned}
 R_s &= \max\{0, I(y_b; s_{km}^l) - I(y_e; s_{km}^l)\} = I(y_b; s_{km}^l) \\
 &= I(y_b; s_m^l).
 \end{aligned}
 \tag{23}$$

5.2 Constellation rotation pattern

As shown in [33], WFRFT is capable of declining the recognition probability of the eavesdropper due to change signal characteristics by adjusting the transform order, which has high potential in anti-recognition. However, some limitations of the existing hybrid carrier systems have emerged. On the one hand, the parameters that can be selected for the disguise of the signal characteristics are limited, which has an adverse effect on the promotion of security. On the other hand, there is no specific analytical solution to the constellation transformation general rules in the literature, thus lacking guidance in practical signal concealment applications. To illustrate the constellation pattern features and improve the performance, in this subsection, three propositions are proved and we introduce the special constellations into the field of anti-recognition.

Let the constellation set of the original symbols be $\Omega = \{r_0 e^{j\varphi_0}\}$, and we take non-normalized 4 phase shift keying (PSK) or quadrature amplitude modulation (QAM) as an example to analyze the regular pattern of the constellation. In this case, the initial constellation set is $\Omega_{4-QAM} = \{\sqrt{2}e^{j\frac{\pi}{4}}, \sqrt{2}e^{j\frac{3\pi}{4}}, \sqrt{2}e^{-j\frac{3\pi}{4}}, \sqrt{2}e^{-j\frac{\pi}{4}}\}$. As shown in Fig. 4, the constellation can be expressed as $\Omega_{GWFRFT} = \{\omega_0^+ x_1 + \omega_2^+ x_2 | x_1, x_2 \in \Omega_{4-QAM}\}$. In

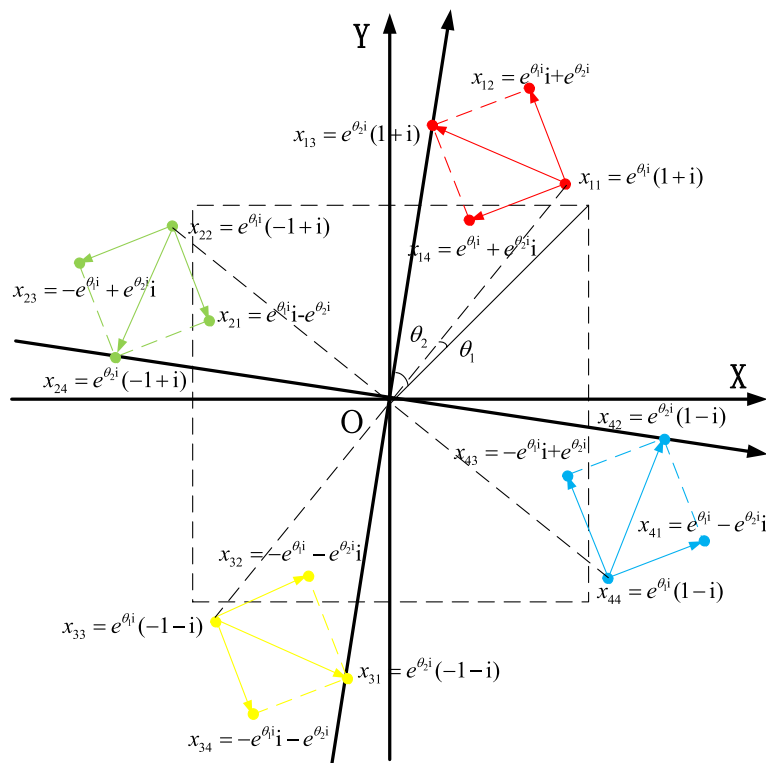


Fig. 4 Constellation pattern of GWFRFT

Table 1 Coordinate expression in Euler's formula

Constellation	x_1	x_2	x_3	x_4
x_1	$x_{11} = e^{\theta_1 i}(1 + i)$	$x_{12} = e^{\theta_1 i j} + e^{\theta_2 i}$	$x_{13} = e^{\theta_2 i}(1 + i)$	$x_{14} = e^{\theta_1 i} + e^{\theta_2 i j}$
x_2	$x_{21} = e^{\theta_1 i j} - e^{\theta_2 i}$	$x_{22} = e^{\theta_1 i}(-1 + i)$	$x_{23} = -e^{\theta_1 i} + e^{\theta_2 i j}$	$x_{24} = e^{\theta_2 i}(-1 + i)$
x_3	$x_{31} = e^{\theta_2 i}(-1 - i)$	$x_{32} = -e^{\theta_1 i} - e^{\theta_2 i j}$	$x_{33} = e^{\theta_1 i}(-1 - i)$	$x_{34} = -e^{\theta_1 i} - e^{\theta_2 i j}$
x_4	$x_{41} = e^{\theta_1 i} - e^{\theta_2 i j}$	$x_{42} = e^{\theta_2 i}(1 - i)$	$x_{43} = -e^{\theta_1 i j} + e^{\theta_2 i}$	$x_{44} = e^{\theta_2 i}(1 - i)$

Table 2 Coordinate expression with θ_1, θ_2

Constellation	x_1	x_2	x_3	x_4
x_1	$(b_1 - a_1, a_1 + b_1)$	$(b_2 - a_1, a_2 + b_1)$	$(b_2 - a_2, a_2 + b_2)$	$(b_1 - a_2, a_1 + b_2)$
x_2	$(-a_1 - b_2, b_1 - a_2)$	$(-b_1 - a_1, b_1 - a_1)$	$(-b_1 - a_2, b_2 - a_1)$	$(-b_2 - a_2, b_2 - a_2)$
x_3	$(a_2 - b_2, -b_2 - a_2)$	$(a_2 - b_1, -a_1 - b_2)$	$(a_1 - b_1, -b_1 - a_1)$	$(a_1 - b_2, -b_1 - a_2)$
x_4	$(b_1 + a_2, a_1 - b_2)$	$(b_2 + a_2, a_1 - b_2)$	$(a_1 + b_2, -b_1 + a_2)$	$(b_1 + a_1, a_1 - b_1)$

the sequel, we use Euler's formula to rewrite the numerical results in Table 1, and we can obtain the coordinate expression in Table 2 with rotation angle θ_1, θ_2 as independent variables, where $a_1 = \sin \theta_1, a_2 = \sin \theta_2, b_1 = \cos \theta_1, b_2 = \cos \theta_2$.

Proposition 1 Four groups of three points $(O, x_{12}, x_{14}), (O, x_{21}, x_{23}), (O, x_{32}, x_{34}), (O, x_{41}, x_{43})$ are collinear, respectively.

Proof To prove the three points are collinear, according to the knowledge of plane geometry, we only need to verify the slope relationship satisfies $k_{Ox_{12}} = k_{Ox_{14}}$.

Case 1 Suppose that $\theta_1 + \theta_2 \neq \frac{\pi}{2}$. Then, we need attest $k_{Ox_{12}} = \frac{\sin \theta_2 + \cos \theta_1}{\cos \theta_2 - \sin \theta_1} = \frac{\sin \theta_1 + \cos \theta_2}{\cos \theta_1 - \sin \theta_2} = k_{Ox_{14}}$, i.e., $\cos^2 \theta_2 - \sin^2 \theta_1 = \cos^2 \theta_1 - \sin^2 \theta_2$, Based on Pythagorean identity

$$\cos^2 \theta_2 + \sin^2 \theta_2 = \cos^2 \theta_1 + \sin^2 \theta_1 = 1, \tag{24}$$

Thus, $k_{Ox_{12}} = k_{Ox_{14}}$ is proved.

Case 2 Suppose that $\theta_1 + \theta_2 = \frac{\pi}{2}$, we have $\cos \theta_2 - \sin \theta_1 = 0$, then we have

$$\begin{aligned} \overrightarrow{Ox_{12}} &= (\cos \theta_2 - \sin \theta_1, \sin \theta_2 + \cos \theta_1) \\ &= (0, \sin \theta_2 + \cos \theta_1), \end{aligned} \tag{25}$$

Meanwhile,

$$\begin{aligned} \overrightarrow{Ox_{14}} &= (\cos \theta_2 - \sin \theta_1, \sin \theta_1 + \cos \theta_2) \\ &= (0, \sin \theta_1 + \cos \theta_2). \end{aligned} \tag{26}$$

That means O, x_{12}, x_{14} are all on axis Y.

Similarly, the other three groups are collinear as well and thus the proof is complete. \square

Proposition 2 Parallelograms $\square x_{11}x_{12}x_{13}x_{14}$, $\square x_{21}x_{22}x_{23}x_{24}$, $\square x_{31}x_{32}x_{33}x_{34}$, $\square x_{41}x_{42}x_{43}x_{44}$ are squares.

Proof Given that $\square x_{11}x_{12}x_{13}x_{14}$ is a parallelogram, to prove that it is a square, we only need to validate that its adjacent sides are equal and two adjacent internal angles are 90° .

$$\overrightarrow{x_{11}x_{12}} = (\cos \theta_2 - \cos \theta_1, \sin \theta_2 - \sin \theta_1), \tag{27}$$

$$\overrightarrow{x_{11}x_{14}} = (-\sin \theta_2 + \sin \theta_1, \cos \theta_2 - \cos \theta_1), \tag{28}$$

$$\overrightarrow{x_{13}x_{14}} = (\cos \theta_1 - \cos \theta_2, \sin \theta_1 - \sin \theta_2), \tag{29}$$

$$\begin{aligned} \overrightarrow{x_{11}x_{12}} \cdot \overrightarrow{x_{11}x_{14}} &= -\cos \theta_2 \sin \theta_2 + \sin \theta_2 \cos \theta_1 + \sin \theta_1 \cos \theta_2 \\ &\quad - \sin \theta_1 \cos \theta_1 + \cos \theta_2 \sin \theta_2 - \sin \theta_2 \cos \theta_1 \\ &\quad - \sin \theta_1 \cos \theta_2 + \sin \theta_1 \cos \theta_1 = \vec{0}, \end{aligned} \tag{30}$$

Similarly, we have $\overrightarrow{x_{11}x_{12}} \cdot \overrightarrow{x_{13}x_{14}} = \vec{0}$, i.e., $\angle x_{12}x_{11}x_{14} = \angle x_{13}x_{14}x_{11} = 90^\circ$. At the same time,

$$\begin{aligned} |\overrightarrow{x_{11}x_{12}}| &= \sqrt{(\cos \theta_2 - \cos \theta_1)^2 + (\sin \theta_2 - \sin \theta_1)^2} \\ &= |\overrightarrow{x_{11}x_{14}}|, \end{aligned} \tag{31}$$

Thus, $\square x_{11}x_{12}x_{13}x_{14}$ is a square. In the same way, that $\square x_{21}x_{22}x_{23}x_{24}$, $\square x_{31}x_{32}x_{33}x_{34}$, $\square x_{41}x_{42}x_{43}x_{44}$ are squares can be verified. \square

Proposition 3 $\angle x_{13}Ox_{11} = \angle x_{22}Ox_{24}x_{11} = \angle x_{31}Ox_{33} = \angle x_{42}Ox_{44} = \theta_1 - \theta_2$.

Proof We can calculate the cosine value to determine these angles.

$$\begin{aligned} \cos \angle x_{11}Ox_{13} &= \frac{\overrightarrow{x_{11}x_{12}} \cdot \overrightarrow{x_{11}x_{13}}}{|\overrightarrow{x_{11}x_{12}}| |\overrightarrow{x_{11}x_{13}}|} \\ &= \frac{\Psi_1 \Psi_2 + \Psi_3 \Psi_4}{\sqrt{\Psi_1^2 + \Psi_3^2} \cdot \sqrt{\Psi_2^2 + \Psi_4^2}} \\ &= \cos \theta_1 \cos \theta_2 + \sin \theta_1 \sin \theta_2 \\ &= \cos(\theta_1 - \theta_2), \end{aligned} \tag{32}$$

where $\Psi_1 = \cos \theta_1 - \sin \theta_1, \Psi_2 = \cos \theta_2 - \sin \theta_2, \Psi_3 = \sin \theta_1 + \cos \theta_1, \Psi_4 = \sin \theta_2 + \cos \theta_2$. \square

From the proofs of Propositions 1–3, it can be seen that the rotated constellation is only determined by two rotation factors θ_1, θ_2 . Combined with Fig. 4, θ_1 is the rotation angle of the initial constellations, and θ_2 is the split angle of the initial constellations. In a nutshell, the original QPSK can be split into 9-point pattern or a 16-point constellation similar to 16QAM, due to GWFRFT.

Since the constellation after 2DGWFRFT is very complicated when the row and column coefficients of each row and column transformation are not uniform, unless otherwise stated, the following only considers the regular pattern that is satisfied whilst the row and column coefficient transformation is unified, $\Omega_{2DGWFRFT} = \{\omega_0^+ x_1 + \omega_2^+ x_2 | x_1, x_2 \in \Omega_{GWFRFT}\}$. Therein, we define that as the transformed constellation set. It can be seen from Fig. 5 that the two rotation splitting processes also follow Propositions 1–3, but the more complicated phenomenon is that the second round parameters continue to split and rotate the GWFRFT pattern. Table 3 shows the parameters' selection under different scenarios, where μ describes the number of points in constellation diagrams. GWFRFT pattern can only provide 4-, 9-, and 16-point constellation features, while 2DGWFRFT can provide $5^2 - 16^2$ point constellation features, which is more abundant and free in the number of split points of confusing constellation diagrams. The simulation results show that, on the one hand, the signal can be hidden by changing the physical layer characteristics through the 2DGWFRFT, which makes it difficult to be detected accurately. On the other hand, it can be disguised as a specific signal through parameters design, so that the eavesdropper will misjudge the modulation mode and transform parameters.

The comparison of our scheme with the traditional SM is shown in Fig. 6. In the traditional SM, illustrated in Fig. 6a, a fixed number of information bits are mapped into constellation panels in the 3D signal domain through conventional modulation techniques, thus making the interception of the modulation type a tractable task. Unlike the traditional SM system, as is depicted in Fig. 6b, the proposed 2DGWFRFT-SC-SM preserves the single-link structure without consuming additional artificial perturbation power compared to AN schemes. Furthermore, the active antennas and modulation type change dynamically according to different parameters, which makes it hard for the eavesdropper to know the right constellation mapping design and can guarantee the security of the wireless communication.

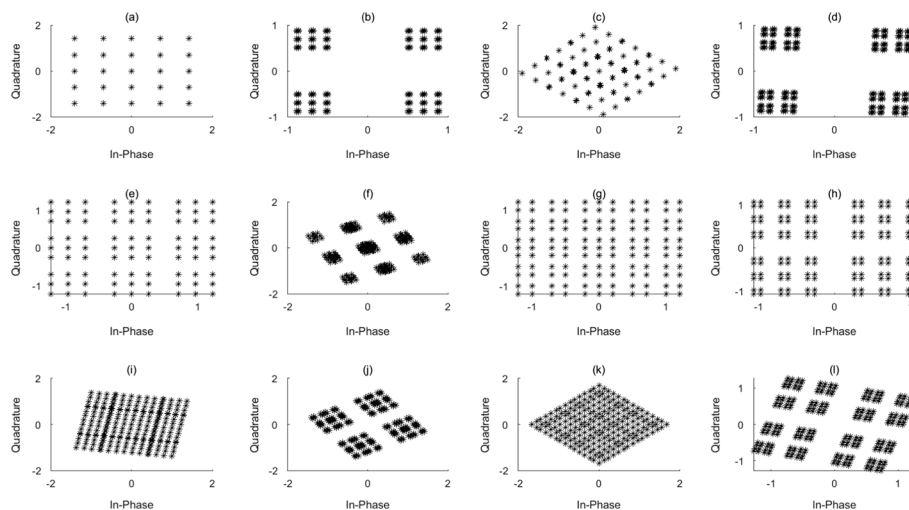


Fig. 5 Special constellation diagrams of 2DGWFRFT

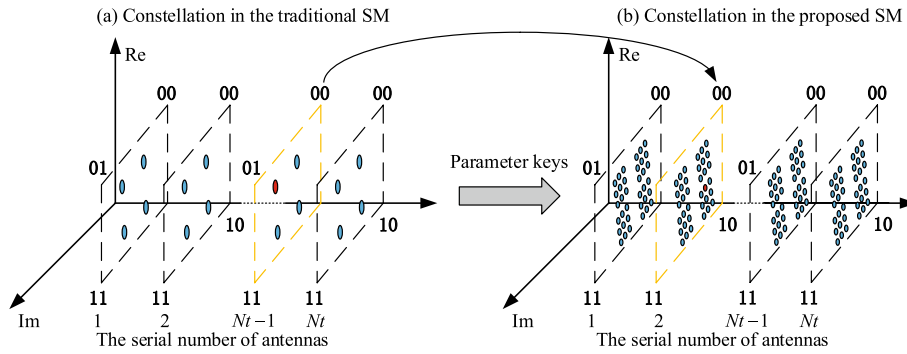


Fig. 6 Constellation diagram comparison between the proposed scheme and the traditional SM

Table 3 Parameter selection under different scenarios in Fig. 5

Figure	(ϕ_0, ϕ_1)	$(\bar{\phi}_0, \bar{\phi}_1)$	μ
(a)	$(\pi/4, 3\pi/4)$	$(3\pi/4, \pi/4)$	$5^2 = 25$
(b)	$(\pi/6, \pi/4)$	$(\pi/4, \pi/3)$	$6^2 = 36$
(c)	$(\pi/5, \pi/2)$	$(\pi/6, 2\pi/3)$	$7^2 = 49$
(d)	$(\pi/5, \pi/4)$	$(\pi/5, \pi/3)$	$8^2 = 64$
(e)	$(0, \pi/6)$	$(\pi/6, 2\pi/3)$	$9^2 = 81$
(f)	$(\pi/5, 2\pi/3)$	$(\pi/6, \pi/4)$	$10^2 = 100$
(g)	$(\pi/4, 0)$	$(3\pi/4, 0)$	$11^2 = 121$
(h)	$(\pi/6, \pi/3)$	$(\pi/6, \pi/3)$	$12^2 = 144$
(i)	$(\pi/5, \pi/2)$	$(\pi/5, 0)$	$13^2 = 169$
(j)	$(\pi/5, \pi/3)$	$(\pi/3, \pi/2)$	$14^2 = 196$
(k)	$(0, \pi/3)$	$(\pi/6, 0)$	$15^2 = 225$
(l)	$(\pi/4, \pi/3)$	$(\pi/4, 0)$	$16^2 = 256$

5.3 Energy efficiency

In MIMO systems, the capacity is directly proportional to the number of antennas. Each antenna is connected to its own RF chain which leads to unnecessary dissipation of power in MIMO communication and incurs additional system costs. SM can be applied to alleviate this issue. By choosing different activation patterns at the transmitter, various SM members provide a flexible design to meet different specific requirements and trade-offs among spectral efficiency, energy efficiency, deployment cost, and system performance [34, 35]. We define the spectral efficiency (SE) as

$$\eta_{SE} = \frac{R_b}{W}, \tag{33}$$

where W represents the bandwidth and the energy efficiency (EE) is given by

$$\Omega_{EE} = \frac{\eta_{SE}}{\omega N_F}, \tag{34}$$

where ω represents the energy consumption of a transmitting symbol and N_F represents the number of RF chains.

In order to make the analysis more comprehensive, we consider the SM-MIMO PLS scheme mentioned in [32, 36, 37] as a contrast. Compared with the scheme in [32], except for Eve’s capacity, the rest of the simulation parameters are the same, which means, our algorithm can achieve a higher secrecy capacity. In the sequel, we will only focus on the comparison between [36, 37] and our scheme. From Table 4, we can see all the simulation parameters. To compare the energy efficiency, we define r_{EE} , r_{SE} and r_{EC} are the ratio of the energy efficiency, spectral efficiency, and energy consumption, respectively, between our scheme and [36]. In [36], all TAs are utilized to transmit modulated signals plus jamming signals. Note that the secrecy enhancement comes at the cost of multiple active RF antennas and excess jamming power. The simulation parameters are the same as our scheme. Obviously, the maximum effective information bits of our scheme (R_1) and the scheme proposed in [36] (R_2) are identical, which are given by

$$R_2 = R_1 = \log_2 M + \log_2 Nt, \tag{35}$$

For this scheme, the secrecy rate increases with the growth of the excess jamming power. Here, we assume that the excess jamming power is equal to the modulated signal power. Assuming there is no error in the transmission process, r_{SE} , r_{EC} , and r_{EE} should be calculated as:

$$r_{SE} = \frac{R_1 W}{R_2 W} = 1, \tag{36}$$

$$r_{EC} = \frac{PT_s}{NtPT_s} = \frac{1}{Nt}, \tag{37}$$

$$r_{EE} = \frac{r_{SE}}{r_{EC}} = Nt. \tag{38}$$

Different from the proposed [36], the novel scheme in [37] only use half of the N antennas to transmit symbols, where the maximum effective information bits (R_3) are given by

$$R_3 = \frac{Nt}{2} (\log_2 M + 1), \tag{39}$$

We define r'_{SE} , r'_{EC} , and r'_{EE} as the ratio of the spectral efficiency, energy consumption, and energy efficiency, respectively, between the 2DGWFRFT-CS-SM scheme and the scheme proposed in [37]. Assuming there is no error in the transmission process, r'_{SE} , r'_{EC} and r'_{EE} should be calculated as:

$$r'_{SE} = \frac{R_1 W}{R_3 W} = \frac{2(\log_2 M + \log_2 Nt)}{Nt(\log_2 M + 1)}, \tag{40}$$

$$r'_{EC} = \frac{PT_s}{\frac{Nt}{2} PT_s} = \frac{2}{Nt}, \tag{41}$$

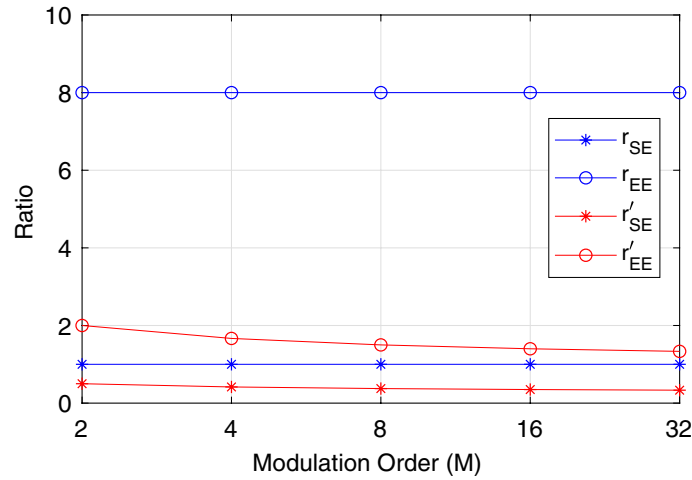


Fig. 7 $r_{SE}, r_{EE}, r'_{SE}, r'_{EE}$ with different modulation order

Table 4 Comparison of conventional SM security algorithms

Parameter	Our scheme	[32]	[36]	[37]
Eve capacity	$R_e \approx 0$	$R_{e1}/Nt + R_{e1}/N$	R_e	–
NF chain	1	1	N_t	$N_t/2$
η_{SE}	$\log_2 NtM/W$	$\log_2 NtM/W$	$\log_2 NtM/W$	$Nt \log_2 M/2W$
Ω_{EE}	$\log_2 NtM/\omega W$	$\log_2 NtM/\omega W$	$\log_2 NtM/\omega WN_F$	$Na \log_2 M/2\omega WN_F$

$$r'_{EE} = \frac{r'_{SE}}{r'_{EC}} = \frac{\log_2 M + \log_2 Nt}{\log_2 M + 1} \tag{42}$$

where P represents the energy required for transmitting each symbol.

The result of r_{SE}, r_{EE}, r'_{SE} , and r'_{EE} with different modulation order and $N = 8$ is depicted in Fig. 7. Compared with the conventional PLS SM system, r_{SE} and r_{EE} remain as modulation order decreases. Note that the r_{EE} is always 8, which means the 2DGW-FRFT-CS-SM scheme has a significant advantage in saving energy at no cost of SE. Compared with the SM-MIMO physical-layer encryption scheme proposed in [37], r'_{SE} and r'_{EE} decrease as modulation order increases. Note that r'_{EE} is always between 1 and 2, while η_{SE} of the 2DGWFRFT-SM scheme is just a little bit lower than the scheme's proposed in [37]. That is to say, our scheme sacrifices a little cost of SE to improve EE, which balances a trade-off between SE and EE.

6 Simulation results

In this section, numerical results are provided to evaluate the proposed method. Without loss of generality, we suppose Bob and Eve have equal noise energy in their received signals, i.e., $\sigma_b^2 = \sigma_e^2$. Additionally, PSK or QAM constellation symbol is adopted and signal-to-noise ratio (SNR) is defined as $1/\sigma_b^2$.

Figures 8 and 9 manifest a comparison of BER performance between legitimate users and eavesdroppers of the proposed scheme. Firstly, in Figs. 8 and 9, Bob's BER

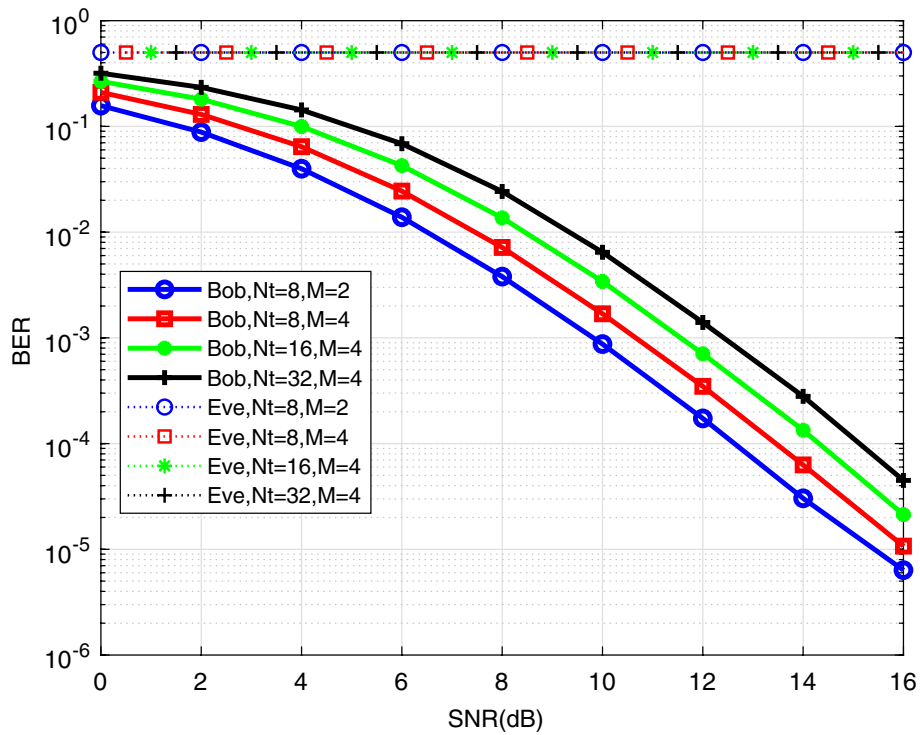


Fig. 8 Performance of BER versus SNR of Bob and Eve for $N_r = N_e = 4$

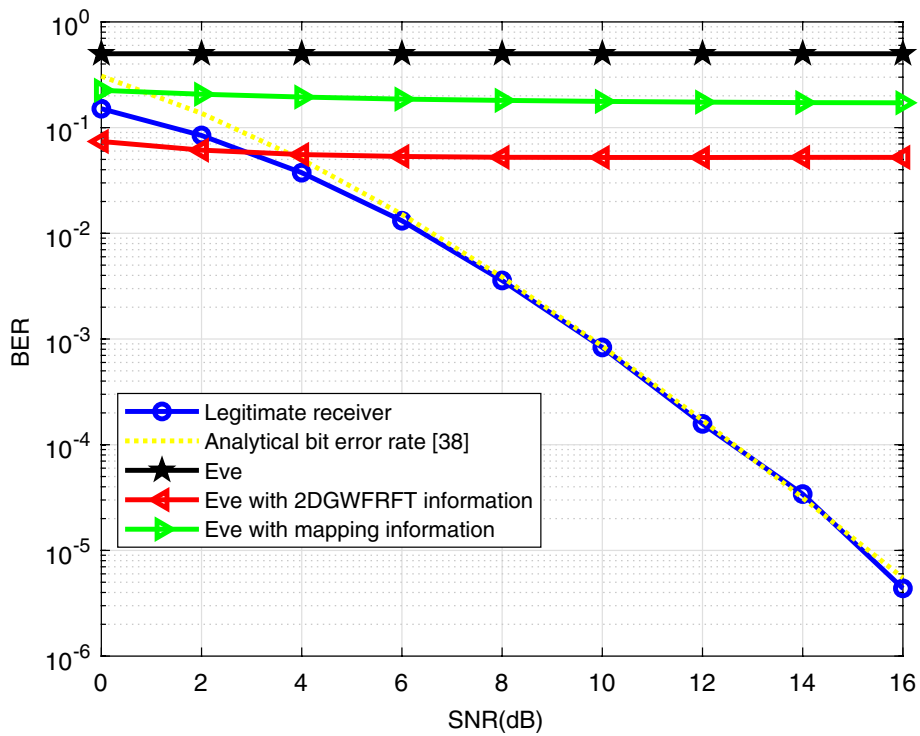


Fig. 9 BER performance of the proposed scheme with analytical result and simulation

decreases rapidly with SNR while Eve’s BER is nearly 0.5 for all SNRs, which indicates that there is no information leaked to Eve from both of the spatial and constellation bits under various numbers of transmit antennas. Secondly, the BER of Bob is very close to that of [38], whereas, for Eve, only about 0.5 BER performance is attained, which means our proposed scheme can drastically increase Eve’s BER at the cost of Bob’s hardly performance loss. Finally, we can observe that in high SNRs, 0.18 for Eve with mapping information and 0.05 for Eve with 2DGWFRFT are achieved, respectively. BER of Eve with mapping information is always worse than the other’s due to the fact that GHC serves more contributions to further deteriorating the signal reception, which has evidently illustrated the inherent PHY security of 2DGWFRFT.

From the perspective of mutual information theory, Fig. 10 depicts the SR comparison of the proposed scheme and WFRFT with different parameters. An interesting phenomenon is observed that except $\Delta\alpha = 0.1$, in other cases the SR is monotonic under low SNR conditions. This phenomenon indicates that in most scenarios the effect of WFRFT parameters is more obvious than SNR. In other words, when parameter difference is minimal, the parameter dominates at low SNRs, while the channel gain takes precedence at high SNRs. What’s more, the 2DGWFRFT curve is always at a high position as a consequence that the SR under this scheme is equal to Bob’s capacity regardless of the parameters.

Figure 11 shows the SR comparison between our proposed scheme and the existing SM-based physical layer security solutions. All schemes are guaranteed to have the same transmission rate of 3 bp/s/Hz. Compared with [39], our proposed approach can achieve an upper bound more quickly at low SNR. We can see that the SR of [11] deteriorates as the number of Eve’s receive antennas increases, contrary to this, our proposed scheme remains constant. The reason for this phenomenon lies in the fact

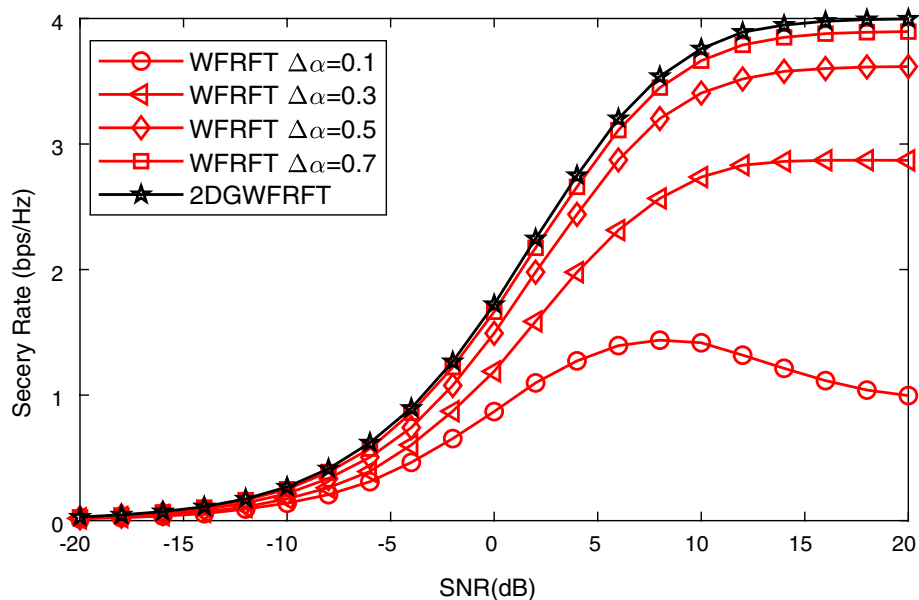


Fig. 10 Secrecy rate comparison of the proposed scheme and WFRFT with $N_e = 1$ under different parameters

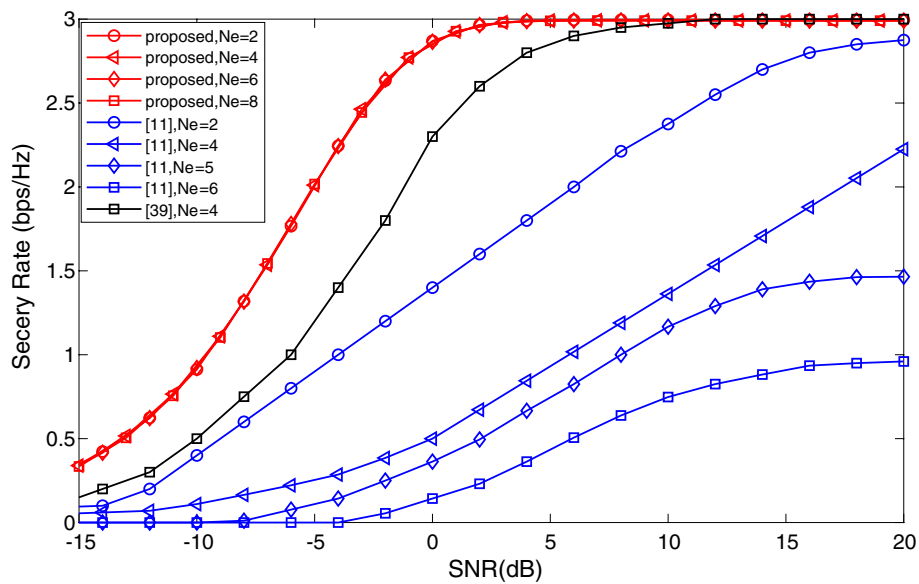


Fig. 11 Secrecy rate comparison with different schemes versus N_e

that the SR obtained by the proposed scheme depends on the superiority provided by 2DGWFRFT, rather than the secrecy of channel gains.

7 Conclusions

We consider the problem of secure communication in the presence of passive eavesdroppers in this paper. In order to enhance the PHY security, we proposed a novel physical layer security scheme based on spatial modulation, whereby both 2DGWFRFT and constellation scrambling method are implemented. The constellation scrambling method can ensure the security, while compared with WFRFT, GWFRFT is extended into a 2D paradigm to provide more freedom of degree in constellation pattern design for the enhanced PHY security provision. Analysis of SR verifies that the proposed scheme can effectively confound the eavesdropper while imposing no impact on the legitimate receivers. Both the theoretical analysis and numerical simulations show that the proposed scheme can achieve a much higher secrecy capacity than AN schemes without requiring additional jamming power consumption.

Abbreviations

AN	Artificial noise
APM	Amplitude/phase modulation
BER	Bit error rate
CS	Constellation scrambling
EE	Energy efficiency
GHC	Generalized hybrid carrier
GWFRFT	Generalized weighted fractional Fourier transform
MIMO	Multiple-input multiple-output
ML	Maximum likelihood
PDF	Probability distribution function
PLS	Physical layer security
PSK	Phase shift keying
PSM	Precoding-aided spatial modulation
QAM	Quadrature amplitude modulation
RF	Radio frequency
SE	Spectral efficiency
SM	Spatial modulation

SNR	Signal-to-noise ratio
SR	Secrecy rate
TA	Transmit antenna
2DGWFRFT	Two-dimensional generalized weighted fractional Fourier transform
WFRFT	Weighted fractional Fourier transform

Acknowledgements

The authors would like to acknowledge all the participants for their contributions to this research study.

Author contributions

YH wrote and edited this manuscript. YH and XS conceptualized this study. XF and GS refined the idea. All authors read and approved the final manuscript.

Funding

The research activities described in this paper have been conducted within the Natural Science Foundation of China under Grant 61901140, in part by the National Key Research and Development Program of China under Grant 2022YFB2902404, in part by the Natural Science Foundation of China under Grant 62171151, in part by the Natural Science Foundation of Heilongjiang Province of China under Grant YQ2021F003, and in part by the Fundamental Research Funds for the Central Universities under Grant HIT.OCEF.2021012.

Availability of data and materials

Not applicable.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

The manuscript does not contain any individual person data in any form (including individual details, images, or videos), and therefore the consent to publish is not applicable to this article.

Competing interests

The authors declare that they have no competing interests.

Received: 18 August 2022 Accepted: 20 December 2022

Published online: 17 January 2023

References

1. C.E. Shannon, Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**(4), 656–715 (1949). <https://doi.org/10.1002/j.1538-7305.1949.tb00928.x>
2. S. Leung-Yan-Cheong, M. Hellman, The gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **24**(4), 451–456 (1978). <https://doi.org/10.1109/TIT.1978.1055917>
3. A.D. Wyner, The wire-tap channel. *Bell Syst. Tech. J.* **54**(8), 1355–1387 (1975). <https://doi.org/10.1002/j.1538-7305.1975.tb02040.x>
4. M. Pei, J. Wei, K.-K. Wong, X. Wang, Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI. *IEEE Trans. Wirel. Commun.* **11**(2), 544–549 (2012). <https://doi.org/10.1109/TWC.2011.120511.110567>
5. L. Dong, Z. Han, A.P. Petropulu, H.V. Poor, Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **58**(3), 1875–1888 (2010). <https://doi.org/10.1109/TSP.2009.2038412>
6. K. Zeng, Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Commun. Mag.* **53**(6), 33–39 (2015). <https://doi.org/10.1109/MCOM.2015.7120014>
7. Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: theories, technologies, and challenges. *IEEE Commun. Surv. Tutor.* **19**(1), 347–376 (2017). <https://doi.org/10.1109/COMST.2016.2598968>
8. R.Y. Mesleh, H. Haas, S. Sinanovic, C.W. Ahn, S. Yun, Spatial modulation. *IEEE Trans. Veh. Technol.* **57**(4), 2228–2241 (2008). <https://doi.org/10.1109/TVT.2007.912136>
9. M.D. Renzo, H. Haas, P.M. Grant, Spatial modulation for multiple-antenna wireless systems: a survey. *IEEE Commun. Mag.* **49**(12), 182–191 (2011). <https://doi.org/10.1109/MCOM.2011.6094024>
10. N. Ishikawa, S. Sugiura, L. Hanzo, 50 years of permutation, spatial and index modulation: from classic RF to visible light communications and data storage. *IEEE Commun. Surv. Tutor.* **20**(3), 1905–1938 (2018). <https://doi.org/10.1109/COMST.2018.2815642>
11. F. Wu, L.-L. Yang, W. Wang, Z. Kong, Secret precoding-aided spatial modulation. *IEEE Commun. Lett.* **19**(9), 1544–1547 (2015). <https://doi.org/10.1109/LCOMM.2015.2453313>
12. F. Wu, C. Dong, L.-L. Yang, W. Wang, Secure wireless transmission based on precoding-aided spatial modulation, in *IEEE Global Communications Conference (GLOBECOM)* (2015), pp. 1–6. <https://doi.org/10.1109/GLOCOM.2015.7417389>
13. F. Wu, R. Zhang, L.-L. Yang, W. Wang, Transmitter precoding-aided spatial modulation for secrecy communications. *IEEE Trans. Veh. Technol.* **65**(1), 467–471 (2016). <https://doi.org/10.1109/TVT.2015.2395457>
14. Y. Chen, L. Wang, Z. Zhao, M. Ma, B. Jiao, Secure multiuser mimo downlink transmission via precoding-aided spatial modulation. *IEEE Commun. Lett.* **20**(6), 1116–1119 (2016). <https://doi.org/10.1109/LCOMM.2016.2549014>

15. L.-L. Yang, Transmitter preprocessing aided spatial modulation for multiple-input multiple-output systems, in *IEEE 73rd Vehicular Technology Conference (VTC Spring)* (2011), pp. 1–5. <https://doi.org/10.1109/VETECS.2011.5956573>
16. X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, X. Shen, On physical layer security: weighted fractional Fourier transform based user cooperation. *IEEE Trans. Wirel. Commun.* **16**(8), 5498–5510 (2017). <https://doi.org/10.1109/TWC.2017.2712158>
17. Q. Cheng, V. Fusco, J. Zhu, S. Wang, F. Wang, WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array. *IEEE Trans. Wirel. Commun.* **18**(11), 5211–5226 (2019). <https://doi.org/10.1109/TWC.2019.2934462>
18. X. Fang, X. Wu, N. Zhang, X. Sha, X. Shen, Safeguarding physical layer security using weighted fractional Fourier transform, *IEEE Global Communications Conference (GLOBECOM)* (2016), pp. 1–6. <https://doi.org/10.1109/GLOCOM.2016.7842239>
19. L. Mei, X. Sha, N. Zhang, The approach to carrier scheme convergence based on 4-weighted fractional Fourier transform. *IEEE Commun. Lett.* **14**(6), 503–505 (2010). <https://doi.org/10.1109/LCOMM.2010.06.092413>
20. J. Lang, R. Tao, Q. Ran, Y. Wang, The multiple-parameter fractional Fourier transform. *Sci. China Ser. F Inf. Sci.* **51**(8), 1010–1024 (2008). <https://doi.org/10.1007/s11432-008-0073-6>
21. C.-C. Shih, Fractionalization of Fourier transform. *Opt. Commun.* **118**(5), 495–498 (1995). [https://doi.org/10.1016/0030-4018\(95\)00268-D](https://doi.org/10.1016/0030-4018(95)00268-D)
22. C. Ma, X. Sha, L. Mei, X. Fang, An equal component power-based generalized hybrid carrier system. *IEEE Commun. Lett.* **23**(2), 378–381 (2019). <https://doi.org/10.1109/LCOMM.2018.2887382>
23. Y. Feng, X. Sha, Y. Li, X. Fang, Y. Zhang, Time-domain dual component computation diversity based on generalized hybrid carrier. *China Commun.* **18**(10), 148–157 (2021). <https://doi.org/10.23919/JCC.2021.10.010>
24. P. Yang, Y. Xiao, Y. L. Guan, K.V.S. Hari, A. Chockalingam, S. Sugiura, H. Haas, M. Di Renzo, C. Masouros, Z. Liu, L. Xiao, S. Li, L. Hanzo, Single-carrier SM-MIMO: a promising design for broadband large-scale antenna systems. *IEEE Commun. Surv. Tutor.* **18**(3), 1687–1716 (2016). <https://doi.org/10.1109/COMST.2016.2533580>
25. Q. Li, M. Wen, M. Di Renzo, Single-RF MIMO: from spatial modulation to metasurface-based modulation. *IEEE Wirel. Commun.* **28**(4), 88–95 (2021). <https://doi.org/10.1109/MWC.021.2000376>
26. U.M. Maurer, Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **39**(3), 733–742 (1993). <https://doi.org/10.1109/18.256484>
27. N. Patwari, J. Croft, S. Jana, S.K. Kasper, High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Trans. Mob. Comput.* **9**(1), 17–30 (2010). <https://doi.org/10.1109/TMC.2009.88>
28. C. Chen, M.A. Jensen, Secret key establishment using temporally and spatially correlated wireless channel coefficients. *IEEE Trans. Mob. Comput.* **10**(2), 205–215 (2011). <https://doi.org/10.1109/TMC.2010.114>
29. H. Liu, J. Yang, Y. Wang, Y. Chen, C.E. Koksal, Group secret key generation via received signal strength: protocols, achievable rates, and implementation. *IEEE Trans. Mob. Comput.* **13**(12), 2820–2835 (2014). <https://doi.org/10.1109/TMC.2014.2310747>
30. S.N. Premnath, S. Jana, J. Croft, P.L. Gowda, M. Clark, S.K. Kasper, N. Patwari, S.V. Krishnamurthy, Secret key extraction from wireless signal strength in real environments. *IEEE Trans. Mob. Comput.* **12**(5), 917–930 (2013). <https://doi.org/10.1109/TMC.2012.63>
31. H. Wang, W.-Q. Wang, S. Ji, Joint precoding spatial and rotating symbol modulation for physical-layer security. *IEEE Commun. Lett.* **23**(12), 2150–2153 (2019). <https://doi.org/10.1109/LCOMM.2019.2944910>
32. Y. Yang, M. Guizani, Mapping-varied spatial modulation for physical layer security: transmission strategy and secrecy rate. *IEEE J. Sel. Areas Commun.* **36**(4), 877–889 (2018). <https://doi.org/10.1109/JSAC.2018.2824598>
33. G. Song, X. Fang, X. Sha, Design and analysis of the EWFRFT-based extended hybrid carrier system, in *International Wireless Communications and Mobile Computing (IWCMC)* (2021), pp. 1162–1167. <https://doi.org/10.1109/IWCMC.51323.2021.9498899>
34. M. Wen, B. Zheng, K.J. Kim, M. Di Renzo, T.A. Tsiftsis, K.-C. Chen, N. Al-Dhahir, A survey on spatial modulation in emerging wireless systems: research progresses and applications. *IEEE J. Sel. Areas Commun.* **37**(9), 1949–1972 (2019). <https://doi.org/10.1109/JSAC.2019.2929453>
35. D. Sinanović, G. Šišul, A.S. Kurdija, Ž. Ilić, Multiple transmit antennas for low PAPR spatial modulation in SC-FDMA: single vs. multiple streams. *EURASIP J. Wirel. Commun. Netw.* **2020**(9), 1–15 (2020). <https://doi.org/10.1186/s13638-020-01669-6>
36. L. Wang, S. Bashar, Y. Wei, R. Li, Secrecy enhancement analysis against unknown eavesdropping in spatial modulation. *IEEE Commun. Lett.* **19**(8), 1351–1354 (2015). <https://doi.org/10.1109/LCOMM.2015.2440353>
37. S. Wang, W. Li, J. Lei, Physical-layer encryption in massive MIMO systems with spatial modulation. *China Commun.* **15**(10), 159–171 (2018). <https://doi.org/10.1109/CC.2018.8485478>
38. R. Mesleh, A. Alhassji, *Space Modulation Techniques* (Wiley, Hoboken, 2018)
39. X.-Q. Jiang, M. Wen, H. Hai, J. Li, S. Kim, Secrecy-enhancing scheme for spatial modulation. *IEEE Commun. Lett.* **22**(3), 550–553 (2018). <https://doi.org/10.1109/LCOMM.2017.2783955>

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.